



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/046,167	01/16/2002	Dai Watanabe	500.41083X00	2273

20457 7590 10/05/2005

ANTONELLI, TERRY, STOUT & KRAUS, LLP
1300 NORTH SEVENTEENTH STREET
SUITE 1800
ARLINGTON, VA 22209-3873

EXAMINER

DADA, BEEMNET W

ART UNIT PAPER NUMBER

2135

DATE MAILED: 10/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/046,167

Applicant(s)

WATANABE ET AL.

Examiner

Beemnet W. Dada

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 January 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-19 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-19 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
- ☒ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 1/16/02.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-19 have been examined.

Double Patenting

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

3. Claims 1-7 and 11-19 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 20-35 of copending Application No. 10/124,577. Although the conflicting claims are not identical, they are not patentably distinct from each other because all elements of claims 1-7 and 11-19 of the present application correspond to claims 20-35 of the copending application, except in the copending application the claims are a program product claims comprising codes to implement elements of the claims. However, It would have been obvious to one having ordinary skill in the art to recognize that method, apparatus, computer program product, etc., claims are equivalent.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 1-19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

6. Claims 1 and 8-10 are directed to an apparatus or a program for generating pseudorandom number. The examiner respectfully asserts that the claimed subject matter does not fall within the statutory classes listed in 35 USC 101. Thus, while the claimed invention may be labeled as an apparatus/program it is in fact functional descriptive material (i.e., computer program, see for example specification page 3, lines 16-20, page 16, lines 5-9 and page 33, lines 1-5). Claims 1 and 8-10 are rejected as being functional descriptive material (i.e., computer program). Claims 2-7 and 11-19 depend on claims 1 and are rejected under the same rationale.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1, 7-10, 14 and 19 are rejected under 35 U.S.C. 102(b) as being anticipated by Daemen et al "Fast Hashing and Stream Encryption with PANAMA" Ref U (hereinafter Daemen).

Art Unit: 2135

9. As per claims 1, 8-10, 14 and 19, Daemen teaches a pseudorandom number generating apparatus wherein said pseudorandom number generating apparatus comprises:

- a state storage section (i.e., 544-bit state, see page 61, section 2);

- a buffer (i.e., 8192 bit buffer, see page 61, section 2);

- a state transformation section for conducting transformation using a storage content of said buffer and a storage content of said state storage section and outputting a result of the transformation (see for example, state updating transformation pages 65-66, section 4.1 and page 61, section 2);

- a state storage control section for updating an internal state of said state storage section by using the output of said state transformation section according to a clock (see for example page 62, state update transformation and figure 1, state updating transformation); and

- a buffer control section for updating an internal state of said buffer by using the output of said buffer transformation section, said state storage section has a capacity of 3 blocks (where one block has n bits), and said buffer has a capacity of a plurality of blocks (see for example page 62, buffer update operation and figure 2), and

- said state transformation section comprises:

- a nonlinear transformation section that uses the storage content of said buffer and the storage content of said state storage section as inputs (page 61, section 2, 2nd paragraph, pages 65 and 66, section 4.1); and

- an output section for outputting one block data included in said result of the transformation as a partial random number sequence [page 61, section 2, last paragraph and page 65-66 section 4.1].

Art Unit: 2135

10. As per claim 7, Daemen further teaches the method wherein said buffer has a capacity of 32 blocks, and said buffer transformation section comprises a processing section for conducting the steps of: outputting blocks included in 32 blocks output by said buffer except a 25th high-order block and a 32nd high-order block, as blocks lowered in order by one; conducting an exclusive OR-ing operation on the 32nd block with its high-order bits and its low-order bits interchanged and the 25th block, and outputting a result of the operation as a 24th block; and conducting an exclusive OR-ing operation on the 32nd block and one block output from the state storage section, and outputting a result of the operation as a 1st block (see figure 2).

Allowable Subject Matter

11. Claims 2-6, 11-13 and 16-18 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims and further rewritten to overcome the rejections under 35 U.S.C 101 and double patenting rejection as indicate above.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO form 892.

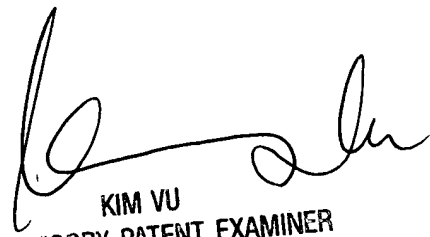
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W. Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada

September 29, 2005



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

INFORMATION UNDER 37 CFR 1.56(a)

(For Initial Filing)

The following references are submitted as information
to comply with the duty of disclosure under 37 CFR 1.56(a):

References	Disclosed in the specification?		Copy			Translation	
	Yes	No	Enc.	Follow	Please obtain	Enc.	Not available
Bp 1. J. Daemen and C. Clapp, "Fast Hashing and Stream Encryption with PANAMA," Fast Software Encryption, 5th International Workshop, Proceedings, LNCS1372, 61-74, Springer-Verlag, 1998.	x		x				
Bp 2. U.S. Patent No. 5,454,039	x		x				
Bp 3. B. Schneier, "Applied Cryptography," John Wiley & Sons, Inc., 1996, pp. 369-428.	x		x				
Bp 4. B. Schneier and D. Whiting, "Fast Software Encryption: Designing Encryption Algorithms for Optimal Software Speed on the Intel Pentium Processor," Fast Software Encryption, 4th International Workshop, FSE'97, Haifa, Israel, January 1997, Proceedings, Lecture Notes in Computer Science, Vol. 1267, Springer-Verlag, pp. 242-259, 1998.	x		x				
Bp 5. J. Daemen and V. Rijmen, "AES Proposal: Rijndael," The first AES Candidate Conference	x		x				

Beemnet Dader 9/28/05